IPEA
EPO
D-80298 Munich
Germany

18th November 2005

Dear Sirs

PCT/GB2004/004701
Our ref: Identities (PCT)

Thank you for the Written Opinion of the ISA.

The Written Opinion cites the following against the independent claims:

D1 US 2003/041154 (Tran Trung)

D2 JSR 118 Expert Group ('Mobile information device profile')

D3 WO 99/44137 (Sun)

Claim 1 reads:

1. A method of controlling access to a specific resource on a mobile telephone; comprising the steps of:

(a) associating an identity with a permission state, in which an identity is a label applicable to one of several entities on whose behalf the resource could potentially be used and the permission state defines whether or not the resource can actually be used; and

(b) allowing use of the resource solely to an entity or entities labelled with an identity associated with a permission state that does permit such use.

The present invention requires that the permission state of an entity is not determined by looking directly at that entity. Instead, another descriptor, called the 'identity' is looked at instead. Counter-intuitively, this leads to a more code efficient access control approach than any of the prior art.

Origin Limited
Twisden Works, Twisden Road, London NW5 1DN
E-mail: peter.langley@origin.co.uk
Tel: +44 (0)20 7424 1950 Fax: +44 (0)20 7209 0643
www.origin.co.uk Registration no. 2211999

For example, in **D1** (see paras 41 and 45, as indicated by the examiner), access control lists are used; these must list every user that has the right to access a given data source. There are different lists for every data source. Hence, for a large firm with 10,000 employees, all needing to access an address book listing all employees contact details, there would be an access control list that defines access to the address book; this will list all 10,000 employees. For another firm resource, perhaps a firm newsletter for all managerial staff, there would be another access control list, again listing all managers that are to be given access to the newsletter.

With the present invention however, employees might be given an identity 'employee'. Then, when an employee makes a request to access some data on another user's mobile telephone, the telephone merely has to determine the permissions associated with the identity presented, i.e. the identity 'employee'. There is no need to store in the telephone the user **IDs** of all employees.

The examiner accepts that **D2** is not directly relevant to the concept of an 'identity' as defined, so we will not consider it in detail here. **D3** is also not relevant either: in **D3**, as in **D1**, access is based on knowledge of the entity requesting access. This is called the 'source' in **D3**:

> "The permissions authorise particular types of access to the resource based on a *source* of the code and an executor of the code" page 6 lines 15 – 16.

D3 would, like **D1**, be very inefficient and not at all suitable for a mobile telephone, where memory constraints are very acute.

Hence, the present invention solves the technical problem of a code efficient way of implementing a permissions based access policy. None of the cited art discloses or suggest the idea of 'identities' on which the present invention is based. Because an identity can define a class of entities, it removes the need to individually list those entities belonging to that class. This in turn greatly reduces the amount of information needed to determine access to a resource, since the decision can be based on the abstraction called an 'identity', rather than the specifics of an individual's ID.

In the light of the above arguments, re-consideration of the present application is requested. Should the examiner require further clarification, a further Written Opinion is requested.

Yours faithfully,

Peter Langley